Talos Labs — Milestone Dossier

Date: 2025-09-18
Project: Modular low-latency agent orchestration prototype
Author: Brandon / Talos Labs — taloslabs2025@proton.me
Archive link: [ADD_ARCHIVE_LINK_HERE]

Executive Summary:
Talos Labs developed a reproducible research prototype demonstrating a modular agent orchestration approach for low-latency coordination. The release is open and archived to ensure transparency. We seek responsible collaboration for independent audit, governance, and safe deployment pathways.

Technical Overview:
Architecture: modular agents, message bus (mocked), orchestration layer, sandbox controls. Minimal dependencies; demo uses simulated inputs.

Capabilities:
- Coordinated message passing in a sandboxed environment.
- Composable orchestration logic for higher-level workflows.

Limitations:
- Network stacks and external integrations are intentionally omitted.
- No credentialed access or real data is included.

Threat Model & Mitigations:
- Harmful automation via uncontrolled composition → sandboxing and rate-limits.
- Sensitive connector leakage → connectors removed/replaced with mocks.

Included Safety Measures:
- Sandbox-only reproduction; sanitized data.
- Responsible disclosure contact and 90-day coordination policy.

Engagement Flow:
1) Verify checksum & archive link.
2) Request controlled access via taloslabs2025@proton.me.
3) Share findings asynchronously; schedule secure call as needed.